The Army Research and Technology Protection Center

U.S. Army Foreign Disclosure Conference

Supporting the Warfighter

30 November 2005

Army Research and Technology Protection Center

The ARTPC is a G-2 funded initiative to integrate and coordinate technology protection activities Army-wide. Directed by a HQ Team of functional protection experts; technology protection engineers (TPEs) are placed on the staffs of key nodes across the Army R&D and acquisition community to provide *dedicated*, *skilled* protection planning support.

Establish a Consistent Process and Standard for Technology Protection within the Army

ARTPC established October 2002

The DCS, G-2 will-

Establish and operate an Army, Research, and Technology Protection Center to integrate and synchronize security, intelligence, counterintelligence, foreign disclosure, and security countermeasure support to research and technology protection activities Army-wide.

AR 70-1 Army Acquisition Policy (31 December 2003)

Mission

ENSURE FUTURE FORCE "CROWN JEWELS" ARE NOT COMPROMISED

- **INTEGRATE AND COORDINATE TECHNOLOGY AND PROGRAM PROTECTION ACTIVITIES ARMY-WIDE**

- **DEVELOP AND IMPLEMENT A CONSISTENT METHODOLOGY FOR THE IDENTIFICATION AND PROTECTION OF CRITICAL PROGRAM AND S&T INFORMATION**

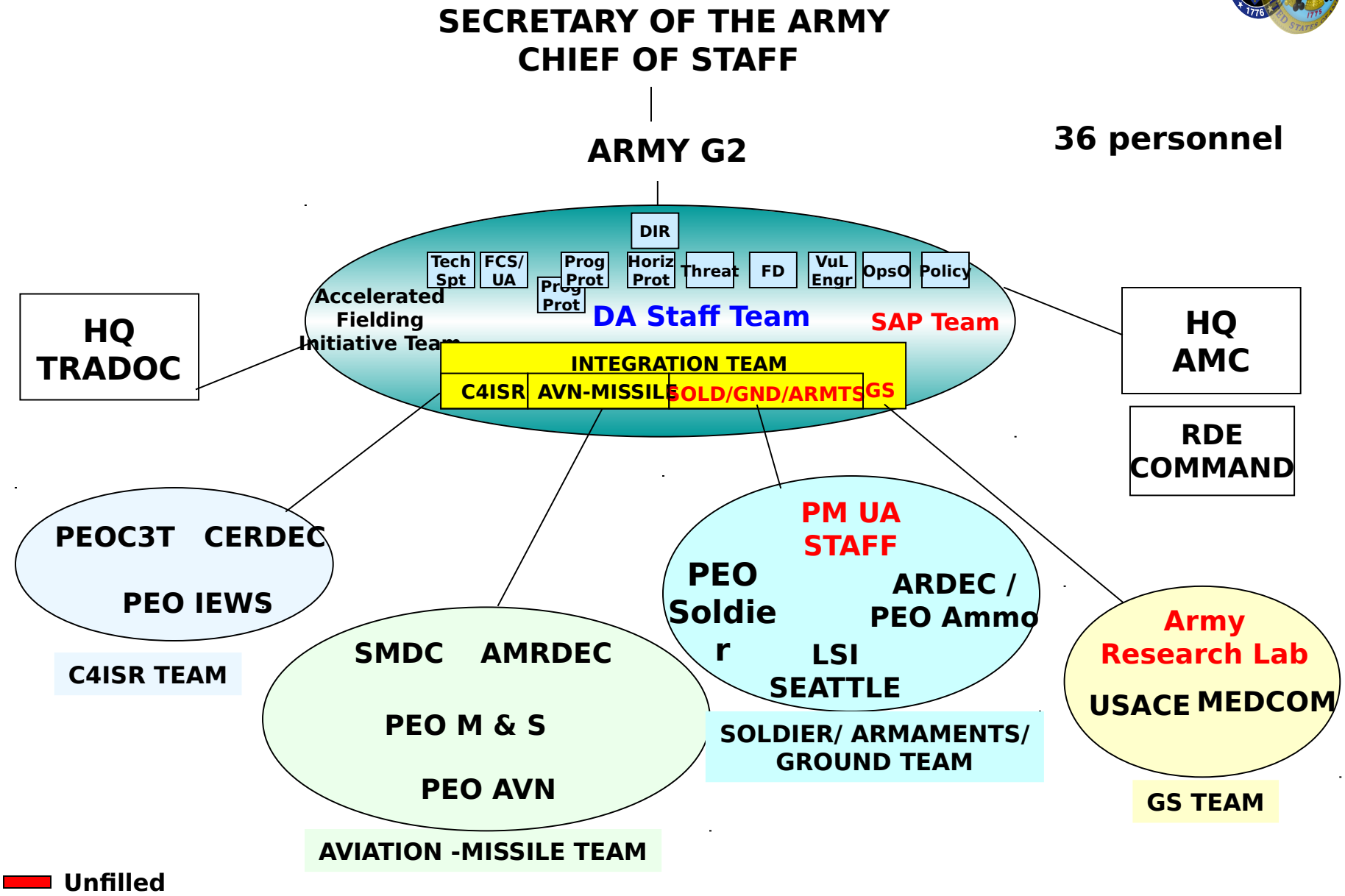
- **IMPROVE THE QUALITY OF INDIVIDUAL AND TEAM PROTECTION IN THE RDECS AND ACQUISITION PROGRAMS**

- **CONDUCT CONTINUOUS SYSTEMIC ANALYSIS AND IMPROVEMENT OF ARMY PROTECTION PROCESSES**

- **PERFORM QUALITATIVE REVIEWS OF TECHNOLOGY AND PROGRAM PROTECTION PLANS TPP / PPP**

- **PROVIDE EXPERT TRAINING**

THE ARMY RESEARCH & TECHNOLOGY PROTECTION CENTER



Center Skill Sets

Technical- Education/Experience

- Physics
- Chemistry
- Mathematics
- Electrical Engineering
- Mechanical Engineering
- Aeronautical Engineering
- Information Technology
- Nuclear Engineering
- Industrial Engineering
- Engineering Management
- System Security Engineering

Security/Intelligence/Law Enforcement

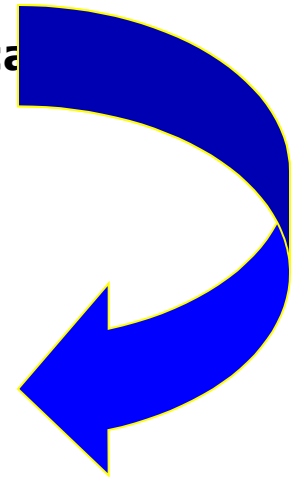
- Program Protection
- SAP Security
- Information Scty
- Personnel Security
- Information Assurance
- Foreign Disclosure/International Programs
- Classification Management
- Industrial Security
- Physical Security
- Anti-terrorism
- OPSEC
- Threat Analysis
- CI Threat Analysis
- Tactical Intelligence
- CI Operations
- Operational Intelligence
- HUMINT
- Strategic Intelligence
- Law Enforcement
- Asset Protection

Army Approach to Tech Protect

- ***Risk Management vs. Risk Avoidance***

- **Develop Army Standard Technology Protection Methodology**

  1. **Critical Program Information (CPI) Identifica**
  2. **Identify Threats**
  3. **Identify Vulnerabilities**
  4. **Conduct Risk Analysis**
  5. **Develop and Implement Countermeasures**



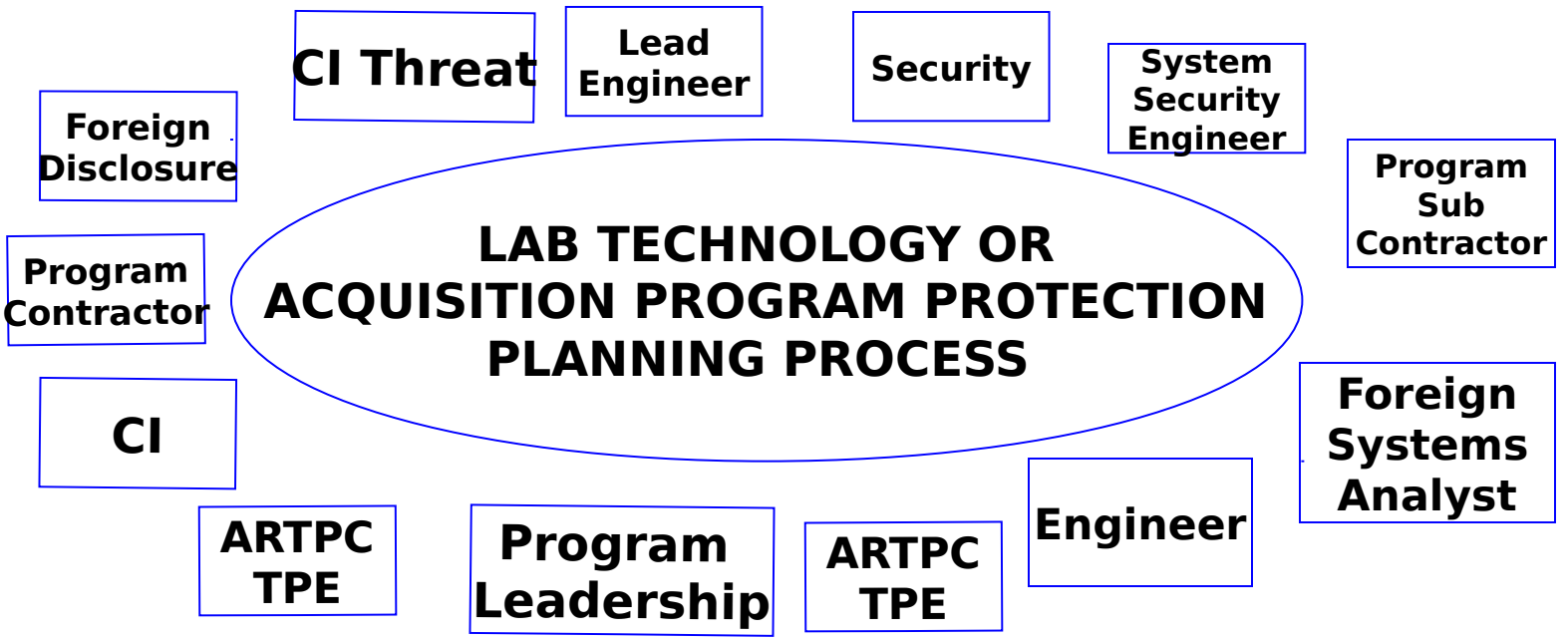
- **Tool Set to support methodology**
  - **CPI Assessment Process**
  - **Susceptibilities Determination**
  - **Vulnerability Analysis Model**
  - **Countermeasures Development/Selection process**
  - **Classification Management Tools**

- **Process executed through Program led Tech Protect IPT**

- **Horizontal integration/synchronization of protection**

- **Formal Review of Protection Plans at HQDA G-2**

Integrated Protection Team

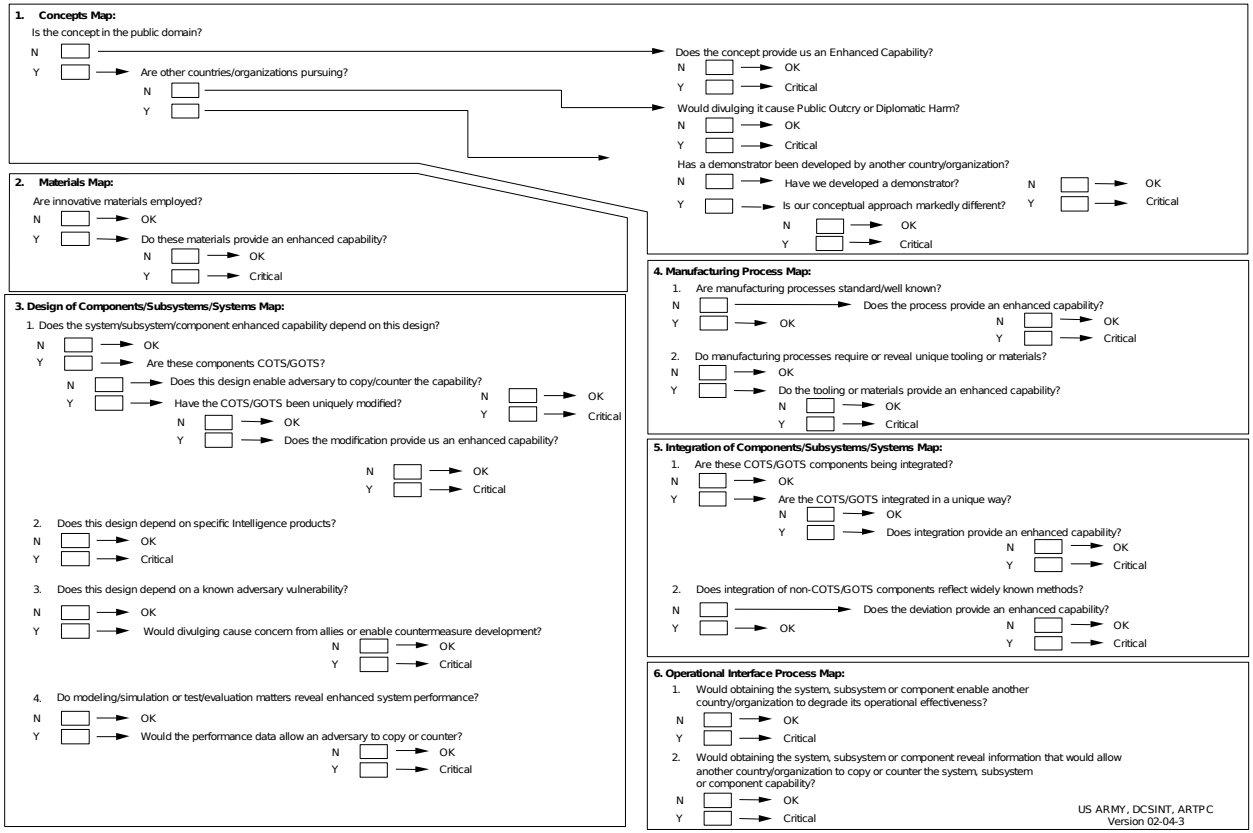


- **Program leads, ARTPC facilitates**
- **In-depth analysis of program technical details and protection requirements**
- **<u>Program identifies CPI and selects countermeasures</u>**

CPI Identification Tool

Provides Framework for discussion leading to ID of CPI

- **Concepts**
- **Materials**
- **Design**
- **Manufacturing**
- **Integration**
- **Operational**


1. Concepts Map:
Is the concept in the public domain?
N
Y
Are other countries/organizations pursuing?
N
Y
Does the concept provide us an Enhanced Capability?
N → OK
Y → Critical
Would divulging it cause Public Outcry or Diplomatic Harm?
N → OK
Y → Critical
Has a demonstrator been developed by another country/organization?
N → Have we developed a demonstrator?
Y → Is our conceptual approach markedly different?
N → OK
Y → Critical
N → OK
Y → Critical
2. Materials Map:
Are innovative materials employed?
N → OK
Y → Do these materials provide an enhanced capability?
N → OK
Y → Critical
3. Design of Components/Subsystems/Systems Map:
1. Does the system/subsystem/component enhanced capability depend on this design?
N → OK
Y → Are these components COTS/GOTS?
N → Does this design enable adversary to copy/counter the capability?
Y → Have the COTS/GOTS been uniquely modified?
N → OK
Y → Does the modification provide us an enhanced capability?
N → OK
Y → Critical
N → OK
Y → Critical
2. Does this design depend on specific Intelligence products?
N → OK
Y → Critical
3. Does this design depend on a known adversary vulnerability?
N → OK
Y → Would divulging cause concern from allies or enable countermeasure development?
N → OK
Y → Critical
4. Do modeling/simulation or test/evaluation matters reveal enhanced system performance?
N → OK
Y → Would the performance data allow an adversary to copy or counter?
N → OK
Y → Critical
4. Manufacturing Process Map:
1. Are manufacturing processes standard/well known?
N → Does the process provide an enhanced capability?
Y → OK
N → OK
Y → Critical
2. Do manufacturing processes require or reveal unique tooling or materials?
N → OK
Y → Do the tooling or materials provide an enhanced capability?
N → OK
Y → Critical
5. Integration of Components/Subsystems/Systems Map:
1. Are these COTS/GOTS components being integrated?
N → OK
Y → Are the COTS/GOTS integrated in a unique way?
N → OK
Y → Does integration provide an enhanced capability?
N → OK
Y → Critical
2. Does integration of non-COTS/GOTS components reflect widely known methods?
N → Does the deviation provide an enhanced capability?
Y → OK
N → OK
Y → Critical
6. Operational Interface Process Map:
1. Would obtaining the system, subsystem or component enable another country/organization to degrade its operational effectiveness?
N → OK
Y → Critical
2. Would obtaining the system, subsystem or component reveal information that would allow another country/organization to copy or counter the system, subsystem or component capability?
N → OK
Y → Critical
US ARMY, DCSINT, ARTPC
Version 02-04-3

A2C2S

ACS

ADOCS

AFATDS

ALES

AN/AVR-2A/B LDS

AN-PPS5D PIP

Apache Avionics,

Apache Block I & II & III TADS

Apache Block III

Apache Block III Fire Control Radar

Apache Longbow Selct Designs

ARL

ASAS Light

ASET IV

ATIRCM

Avenger

Avenger FLIR Upgrade

BBM

Blackhawk UH/HH-60M

CAP Combined Aggregate Program

CDA

Centaur

CGS/JSWS

CHIMS

Chinook CH-47F

CID

Comanche-TUAV Linkage

DAGR

DCGS-A

DVE

ENVG

EO/IR/LD

FBCB2

FCS

GB-GRAM

GCCS-A

GRCS

HTI 2ND Gen FLIR

IBCS

JMT

JMETS

JCM

JLENS (Spiral 2)

JLENS RAID (Spiral 1)

JNMS

JSSEO IABM

JTAGS

JTRS CI 1

JTRS CI 5

JTT

LOSAT

LRAS3

Lynx1

MBCOTM

MEADS

MTHEL

NLOS-LS

NOC-V

PAC-3

PATRIOT Legacy

PFED

Phoenix BSS

PLGR

Profil

Q

PSDS2

PTDS

REMBASS II

SAR/GMTI

SBA for ACS

SENTINEL

Shortstop/SEPS

SIRFC

SLAMRAAM

SWLAN

Tactical LIDAR

Tactical SIGINT Payload

TENCAP

TES

THAAD (MDA)

UGS

Uncooled B Kit

Warlock

WIN-T

WSS

XM08

160+ PROGRAM ASSESSMENTS

Classification Methodology

Eligibility

- **Is the information classified by another program?**
- **Is the information under control of U.S. government?**
- **Does information fall under category identified in AR 380-5?**

Determination

- **Asks a series of questions designed to differentiate AR 380-5 standards**
  - **“Damage”**
  - **“Serious Damage”**
  - **“Grave Damage”**

Establish a Consistent Process and Standard for Technology Protection within the Army

Classification Management Support

- An/ARC-220 High Frequency Radio System
- A2C2S
- ABCS
- ACS
- Apache
- Aviation Mission Planning System (AMPS)
- CH-47F
- EMG
- Excalibur
- FBCB2
- Future Cargo Aircraft
- FCS and FCS Family of System (developed)
- Gunslinger (Marine Corps)
- Interceptor Body Armor
- IBCS
- Joint Common Missile
- JLENS (developed)
- JSSEO
- JTRS Cluster 2 (SOCOM))
- Lightweight Modular Causeway formally RPE
- NLOS
- JTDS
- REMBASS II
- Soldier Radio Waveform (SRW) (developed)
- Solid State Heat Capacity Laser
- Stryker
- SLAMRAAM
- Thermal Weapon Sight (TWS)
- Weapon Surveillance System (WSS) (developed)

30+ SCG's developed/revised

Establish a Consistent Process and Standard for Technology Protection within the Army

Accelerated Fielding Initiative (AFI)

- **Requirement to consider AFI technology for protection prior to deployment**

- **AFI Team provides "start to finish" prgm protection to AFI technologies**

- **Standard protection methodology not responsive enough to support AFI timeline**
  - **planning process compressed as required**
  - **process led by ARTPC, AFI Team develops protection plan**
  - **executes battle handover with gaining unit**

- **Tied to REF, TRADOC, FORSCOM, ATEC, CENTCOM, SOCOM, Joint IEDD TF**

- **End State: Combat capability delivered to the warfighter with tailored Countermeasures, OPSEC Plan, etc.**

- **Primary focus to date- Force Protection- PTDS and Counter JED- Warlock, CREW2**

"Transformation occurs within a context of continuous change. We will provide for the accelerated fielding of select future force capabilities to enable the enhancement of the Current Force."

-Gen Schoomaker-
From "The Way Ahead, Our Army at War... Relevant and Ready" Nov 2003

ARTPC Value Added

- **Support to Technology Manager in technical assessment of SAP candidate for CPI**

- **Visibility on results of ARTPC CPI assessments**

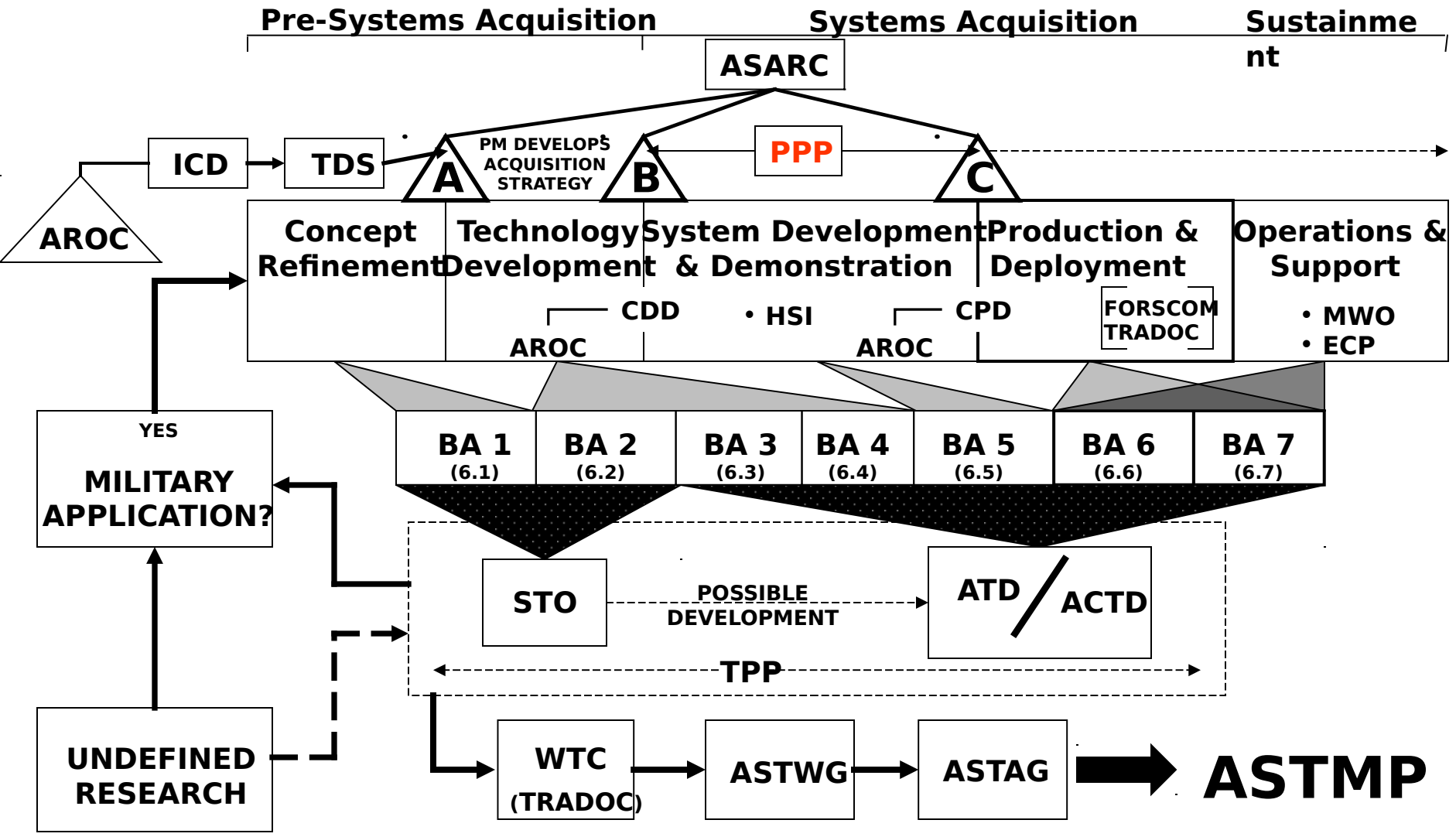
- **Can provide a standardized approach to SCG development**

- **Support SAP transition to collateral-side**

- **“Scouts out” for sensitive technology**

PROGRAM PROTECTION PLANNING
And The
FOREIGN DISCLOSURE OFFICER

US Army R&D and Acquisition



Program Protection Plan

PPP **will address, at minimum, following:**

- **System and Program Description** (PMO)
- **List of CPI** (PMO with HQDA, G-2/ARTPC as facilitator)
- **Threats to CPI** (ACIC)
- **Vulnerabilities of CPI to Threats** (HQDA, G-2/ARTPC)
- **Security Classification Guide** (PMO/Security Manager lead)
- **Countermeasures** (HQDA, G-2/ARTPC)
- **System Security Engineering** (PMO/Security Manager lead)
- **Protection Costs** (PMO/Security Manager lead)
- **Technology Assessment and Control Plan** (PMO/International Program lead)
- **Foreign Sales and Co-Production** (ASA(ALT) lead)
- **Foreign Disclosure** (PMO/Foreign Disclosure lead)

PPP Lessons-Learned

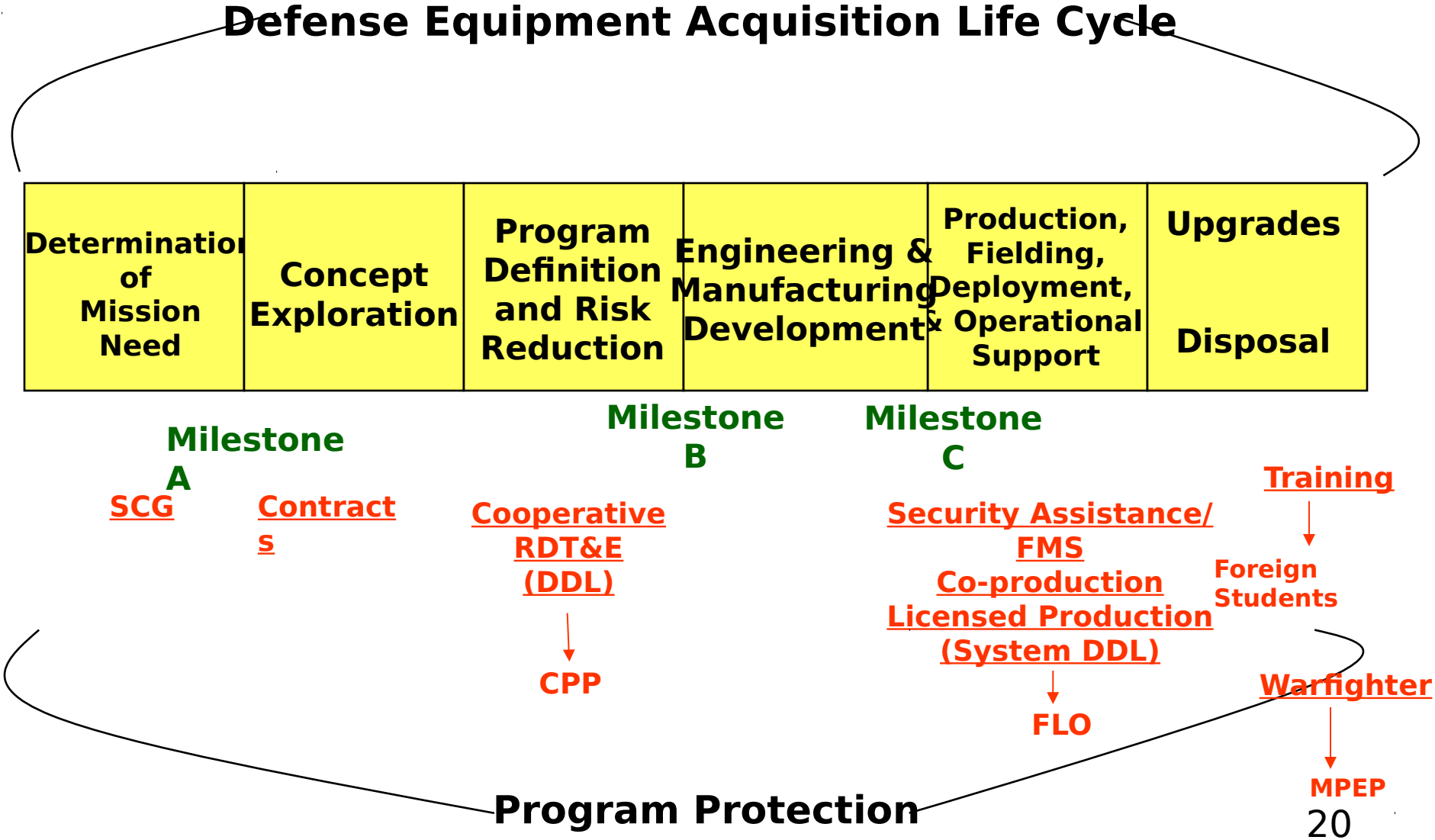
- Security Classification Guides
  - **Unauthorized Original Classification Authority (OCA)**
  - **Incorporation of unauthorized elements, such as COMSEC**
  - **Omission of elements, such as maintenance and training**
  - **Failure to transition OCA with transfer of program**
  - **Failure to review for downgrade and declassification of classified information**
  - **Failure to address non-public domain information**
- Impact on Foreign Disclosure
  - **Delegated disclosure authority (OCA)?**
  - **Assignment of proper security classification levels to data?**
  - **Identification of correct information for disclosure?**

PPP Lessons-Learned

- Horizontal Protection
  - **Security classification level mismatch**
  - **Adoption of inconsistent countermeasures for protection**
  - **Transfer of OCA not addressed in transition**

- Impact on Foreign Disclosure
  - **Consistency of CMI disclosures?**
  - **Incorporation of countermeasures, such as limitations and procedures, in DDL?**

Program Protection Life Cycle



Program Protection Plan

PPP **will address, at minimum, following:**

- **System and Program Description**
- **List of CPI**
- **Threats to CPI**
- **Vulnerabilities of CPI to Threats**
- **Security Classification Guide(s)**
- **Countermeasures**
- **System Security Engineering**
- **Protection Costs**
- *International Government-to-Government Programs*
  - *Technology Assessment and Control Plan (TA/CP)*
  - *Foreign Sales and Co-Production*
  - *Foreign Disclosure*

ARMY RESEARCH AND TECHNOLOGY PROTECTION CENTER

What Are Your Questions?